AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

receiving an encrypted communication at a second transfer point in a second host, the communication sent by a first process to be encrypted by a first transfer point in a first host using an object library, the object library being between a transport layer of network communication and input and output channels, the object library to create stateful objects from objects of application processes for communication between hosts;

decrypting the communication at the second transfer point using the object library; and

transferring the decrypted communication between the second transfer point and a second process within the second host;

wherein a communication channel using the object library between the first transfer point and the second transfer point allows encrypted communication between a plurality of application processes within the first host and a plurality of application processes within the second host.

2. (Original) The method of claim 1, wherein a first plurality of processes are provided within the first host and a second plurality of processes are provided within the second host.

3. (Original) The method of claim 2, wherein the first plurality of processes within the first host can communicate securely with each other and the second plurality of processes within the second host can communicate securely with each other.

4. (Original) The method of claim 3, wherein the first plurality of processes can communicate simultaneously with each other and the second plurality of processes can communicate simultaneously with each other.

5. (Original) The method of claim 1, wherein the encrypted communication is transferred through a connection.

6. (Original) The method of claim 5, wherein the connection is a single-pipe connection.

7. (Currently Amended) A machine-readable storage medium tangibly embodying a sequence of instructions executable by the machine to perform a method, the method comprising the steps of:

receiving an encrypted communication at a second transfer point in a second host, the communication sent by a first process to a first transfer point to be encrypted in a first host using an object library, the object library being between a transport layer of network communication and input and output channels, the object library to create stateful objects from objects of application processes for communication between hosts;

decrypting the communication at the second transfer point using the object library; and

transferring the decrypted communication between the second transfer point and a second process within the second host;

wherein a communication channel using the object library between the first transfer point and the second transfer point allows encrypted communication between a plurality of application processes within the first host and a plurality of application processes within the second host.

8. (Original) The machine-readable medium of claim 7, wherein a first plurality of processes are provided within the first host and a second plurality of processes are provided within the second host.

9. (Original) The machine-readable medium of claim 8, wherein the first plurality of processes within the first host can communicate securely with each other and the second plurality of processes within the second host can communicate securely with each other.

10. (Original) The machine-readable medium of claim 9, wherein the first plurality of processes can communicate simultaneously with each other and the second plurality of processes can communicate simultaneously with each other.

11. (Original) The machine-readable medium of claim 7, wherein the encrypted communication is transferred through a connection.

12. (Original) The machine-readable medium of claim 11, wherein the connection is a single-pipe connection.

13. (Currently Amended) A system comprising:

a first process in a first host; and

a second process in a second host, the second process receiving communication from the first process, the communication having been encrypted by a first transfer point in the first host using an object library and received by a second transfer point within the second host to decrypt the communication using the object library in order to be transferred to the second process, the object library being between a transport layer of network communication and input and output channels, the object library

to create stateful objects from objects of application processes for communication between hosts;

wherein a communication channel established using the object library between the first transfer point and the second transfer point allows encrypted communication between a plurality of application processes within the first host and a plurality of application processes within the second host.

14. (Original) The system of claim 13, wherein a first plurality of processes are provided within the first host and a second plurality of processes are provided within the second host.

15. (Original) The system of claim 14, wherein the first plurality of processes within the first host can communicate securely with each other and the second plurality of processes within the second host can communicate securely with each other.

16. (Original) The system of claim 15, wherein the first plurality of processes can communicate simultaneously with each other and the second plurality of processes can communicate simultaneously with each other.

17. (Original) The system of claim 13, wherein the encrypted communication is transferred through a connection.

18. (Original) The system of claim 17, wherein the connection is a single-pipe connection.

19. (New) The method of claim 1, wherein the object library is to dynamically perform type compatibility determination based on names and behavior version numbers of object types.

20. (New) The method of claim 1, further comprising:

bundling communication of a plurality of processes running inside the first host at the same time for communication to the second host.